# Savitribai Phule Pune University

(Formerly University of Pune)

## Bachelors Degree in Cyber Security

(Faculty of Science and Technology)

# Syllabi for
# B.Sc. (Cyber Security)-Third Year
# Sem-V and VI

(For Colleges Affiliated to Savitribai Phule Pune University)

Choice Based Credit System (CBCS) Syllabus
Under National Education Policy (NEP)

**To be implemented from Academic Year 2026-27**

# Savitribai Phule Pune University

## Syllabus Structure as per NEP Guidelines

## B.Sc. (Cyber Security) from 2026-27

### TY (Level 5.5) SEMESTER V

| Course Type | Course code | Course Name | Credits | | Teaching Scheme Hrs/Week | | Examination Scheme and Marks | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | TH | PR | TH | PR | CE | EE | Total |
| Major Core | CYS-301-MJ-T | Web Application Security | 2 | | 2 | | 15 | 35 | 50 |
| | CYS-302-MJ-T | Vulnerability Assessment | 2 | | 2 | | 15 | 35 | 50 |
| | CYS-303-MJ-T | Basics of API security testing | 2 | | 2 | | 15 | 35 | 50 |
| | CYS-304-MJ-T | Automation in Python for Cyber Security | 2 | | 2 | | 15 | 35 | 50 |
| | CYS-305-MJ-P | Lab Course based on CYS-301-MJ-T & CYS-302-MJ-T | | 2 | | 4 | 15 | 35 | 50 |
| | CYS-306-MJ-P | Lab Course based on CYS-303-MJ-T & CYS-304-MJ-T | | 2 | | 4 | 15 | 35 | 50 |
| Major Elective | CYS-310-MJ-T | Basics of Digital Forensic | 2 | | | | 15 | 35 | 50 |
| | CYS-311-MJ-P | Lab Course based on CYS-310-MJ-T | | 2 | | 4 | 15 | 35 | 50 |
| | | OR | | | | | | | |
| | CYS-312-MJ-T | DevOps Fundamentals | 2 | | 2 | | 15 | 35 | 50 |
| | CYS-313-MJ-P | Lab Course based on CYS-312-MJ-T | | 2 | | 4 | 15 | 35 | 50 |
| VSC | CYS-321-VSC-T | Embedded Systems | 2 | | 2 | | 15 | 35 | 50 |
| FP/CEP | CYS-331-FP | Project on Cyber Security | | 2 | | 4 | 15 | 35 | 50 |
| Minor | CYS-341-MN-T | Internet of Things for Cyber Security | 2 | | 2 | | 15 | 35 | 50 |
| | | **Total** | **14** | **8** | **14** | **16** | | | **550** |

# Savitribai Phule Pune University

## Syllabus Structure as per NEP Guidelines

## B.Sc. (Cyber Security) from 2026-27

### TY (Level 5.5) SEMESTER VI

| Course Type | Course code | Course Name | Credits | | Teaching Scheme Hrs/Week | | Examination Scheme and Marks | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | TH | PR | TH | PR | CE | EE | Total |
| Major Core | CYS-351-MJ-T | Windows Terminal for Cyber Security | 2 | | 2 | | 15 | 35 | 50 |
| | CYS-352-MJ-T | PowerShell basics | 2 | | 2 | | 15 | 35 | 50 |
| | CYS-353-MJ-T | Fundamentals of Active Directory | 2 | | 2 | | 15 | 35 | 50 |
| | CYS-354-MJ-T | Penetration Testing | 2 | | 2 | | 15 | 35 | 50 |
| | CYS-355-MJ-P | Lab Course based on CYS-351-MJ-T & CYS-352-MJ-T | | 2 | | 4 | 15 | 35 | 50 |
| | CYS-356-MJ-P | Lab Course based on CYS-353-MJ-T & CYS-354-MJ-T | | 2 | | 4 | 15 | 35 | 50 |
| Major Elective | CYS-360-MJ-T | Advanced Digital Forensic | 2 | | 2 | | 15 | 35 | 50 |
| | CYS-361-MJ-P | Lab Course based on CYS-360-MJ-T | | 2 | | 4 | 15 | 35 | 50 |
| | | OR | | | | | | | |
| | CYS-362-MJ-T | DevSecOps Fundamentals | 2 | | 2 | | 15 | 35 | 50 |
| | CYS-363-MJ-P | Lab Course based on CYS-362-MJ-T | | 2 | | 4 | 15 | 35 | 50 |
| VSC | CYS-371-VSC | Embedded Systems Programming | | 2 | | 4 | 15 | 35 | 50 |
| OJT | CYS-381-OJT | On Job Training | | 4 | | 8 | 30 | 70 | 100 |
| | | **Total** | **10** | **12** | **10** | **24** | | | **550** |

# Detail Syllabus
# B.Sc. (Cyber Security)
# Semester-V

# Savitribai Phule Pune University
## B.Sc. Cyber Security
## Sem-V

### CYS-301-MJ-T: Web Application security

| No. of Credits: | Teaching Scheme | Examination Scheme |
|---|---|---|
| 2 | Theory: 2 Hrs/Week | Continuous Evaluation: 15 Marks<br>End Semester : 35 Marks |

**Prerequisites**

- Basic knowledge of networking
- Web technologies (HTML, HTTP)
- Cybersecurity fundamentals

**Objectives**

- To understand the architecture and working of web applications.
- To know common web vulnerabilities.
- To study secure coding principles to prevent attacks.
- To study web penetration testing using security tools.
- To apply modern practices for enhanced protection.

**Course Outcomes**

On Completion of this course, student will be able to –
CO1: Understand the architecture and working of web applications.
CO2: Identify and analyze common web vulnerabilities.
CO3: Apply secure coding principles to prevent attacks.
CO4: Perform web penetration testing using security tools.
CO5: Implement modern practices such as DevSecOps and WAF for enhanced protection.

| Unit No. | Name of Unit | Teaching Hours | CO Targeted |
|---|---|---|---|
| **1** | **Introduction to Web Application Security** | **5** | **CO1** |

- Understanding Web Application Architecture (Client, Server, Database)
- HTTP/HTTPS Basics and Communication Flow
- Common Attack Surface in Web Applications
- Importance of Secure Coding Practices
- OWASP and its Role in Web Security
- Overview of OWASP Top 10 Vulnerabilities (2021 edition)
- Web Application Security Testing Life Cycle (WSTLC)
- Learning Outcome: Students understand web app components, vulnerabilities, and security frameworks like OWASP.

| | | | |
|---|---|---|---|
| **2** | **Authentication and Session Management** | **5** | **CO1** |

- Authentication vs Authorization
- Secure Password Storage (Hashing, Salting, PBKDF2, bcrypt)

- Multi-Factor Authentication (MFA)
- Session Management: Cookies, Tokens, and JWT
- Common Attacks: Session Hijacking, Session Fixation, Cookie Poisoning
- Secure Implementation of Login/Logout Mechanisms
- Best Practices for Identity and Access Management (IAM)
- Learning Outcome: Students learn secure methods of managing users and protecting sessions.

| 3 | **Web Application Vulnerabilities and Exploits** | 6 | CO2 |
|---|---|---|---|

- Cross-Site Scripting (XSS): Types and Prevention
- SQL Injection and Database Security
- Cross-Site Request Forgery (CSRF)
- Command Injection and Path Traversal
- Insecure Direct Object Reference (IDOR)
- XML External Entities (XXE)
- Case Studies: Famous Web Security Breaches
- Practical Component: Hands-on demonstration using DVWA / OWASP Juice Shop.
- Learning Outcome: Students identify, exploit (ethically), and patch vulnerabilities in web applications.

| 4 | **Secure Coding and Defensive Mechanisms** | 5 | CO3 |
|---|---|---|---|

- Secure Development Life Cycle (SDLC)
- Input Validation and Output Encoding
- Error and Exception Handling
- Use of Security Libraries and Frameworks
- Content Security Policy (CSP)
- Secure File Upload and Data Storage
- Logging and Monitoring of Web Applications
- Learning Outcome: Students understand secure programming practices and how to integrate them in development.

| 5 | **Web Application Penetration Testing** | 5 | CO4 |
|---|---|---|---|

- Penetration Testing Methodology (Information Gathering to Reporting)
- Reconnaissance and Vulnerability Scanning Tools
- Manual vs Automated Testing
- Tools: Burp Suite, OWASP ZAP, Nikto, Nmap
- Report Writing and Risk Assessment
- Ethical and Legal Aspects of Web Testing
- Learning Outcome: Students can perform and document a basic penetration test ethically and professionally.

| 6 | **Modern Web Security Practices** | 4 | CO5 |
|---|---|---|---|

- Secure APIs and RESTful Security
- Web Application Firewalls (WAFs)

- Cloud-based Web Security Solutions
- HTTPS, TLS/SSL Certificates and HSTS
- Secure DevOps (DevSecOps) Concepts
- Zero Trust Architecture for Web Security
- Security in Single Page Applications (SPA) and Mobile Web
- Learning Outcome: Students explore advanced and modern techniques for securing web apps in cloud and DevOps environments

## Reference Books


- Web Application Hacker's Handbook, by Dafydd Stuttard and Marcus Pinto, Released September 2011,
  Publisher(s): Wiley Publishing, ISBN: 9781118026472.
- OWASP Testing Guide, by OWASP, Released 2021,
  Publisher(s): OWASP Foundation.
- The Tangled Web: A Guide to Securing Modern Web Applications, by Michal Zalewski, Released November 2011,
  Publisher(s): No Starch Press, ISBN: 9781593273880
- Web Security for Developers, by Malcolm McDonald, Released June 2009,
  Publisher(s): O'Reilly Media, ISBN: 9780596802769.
- SQL Injection Attacks and Defense, by Justin Clarke, Released April 2012,
  Publisher(s): Syngress, ISBN: 9781597499637.


## E-Books and Online Learning Material

- **https://owasp.org/www-project-top-ten/?utm_source=chatgpt.com**
- **https://owasp.org/www-project-top-ten/?utm_source=chatgpt.com**

# Savitribai Phule Pune University

## CYS-302-MJ-T : Vulnerability Assessment

| No. of Credits: 2 | Teaching Scheme<br>Theory: 2 Hrs/Week | Examination Scheme<br>Continuous Evaluation: 15 Marks<br>End Semester : 35 Marks |
|---|---|---|

**Prerequisites:** Basic knowledge of HTTP, REST architecture, and web security fundamentals.

**Objectives**

- To study VA methodology, tools, and legal/ethical constraints.
- To discover and enumerate assets using passive and active techniques.
- To study automated vulnerability scans for reducing false positives.
- To study critical vulnerabilities and impact safely.
- To create prioritized remediation plans and reports.
- To integrate VA practices into ongoing security workflows.

**Course Outcomes**

On Completion of this course, student will be able to –

CO1: Explain VA methodology, tools, and legal/ethical constraints.

CO2: Discover and enumerate assets using passive and active techniques.

CO3: Run and interpret automated vulnerability scans and reduce false positives.

CO4: Manually validate critical vulnerabilities and demonstrate impact safely.

CO5: Create prioritized remediation plans and professional VA reports.

CO6: Integrate VA practices into ongoing security/DevOps workflows.

| Unit No. | Name of Unit | Teaching Hours | CO Targeted |
|---|---|---|---|
| 1 | **Fundamentals of Vulnerability Assessment** | 4 | CO1 |

- Definitions: vulnerability, threat, risk, exploit, exposure
- VA vs Penetration Testing vs Risk Assessment
- Vulnerability lifecycle and CVE/CVSS basics
- Types of assets and attack surfaces (network, host, application, cloud, IoT)
- Legal, ethical, and compliance considerations
- Outcome: Understand core concepts and scope of VA.

| | | | |
|---|---|---|---|
| 2 | **Reconnaissance & Information Gathering** | 5 | CO2 |

- Passive vs active reconnaissance
- Open Source Intelligence (OSINT) techniques and tools
- Network discovery: host discovery, service enumeration
- Fingerprinting: OS, services, application versions
- Asset inventory and prioritization
- Practical component: Use Nmap, Netdiscover, and basic OSINT tools.
- Outcome: Collect and prioritize accurate information for assessment.

| | | | |
|---|---|---|---|
| 3 | **Vulnerability Scanning** | 6 | CO3 |

- Types of scanners: network, host, web, database, cloud
- Scanning methodologies: authenticated vs unauthenticated scans
- Popular scanners and their architectures (Nessus, OpenVAS, Qualys, Nexpose)

- Scan tuning, false positives/negatives, credentialed scans
- Interpreting scanner output and vulnerability databases (NVD)
- Practical component: Configure and run scans with OpenVAS / Nessus; analyze results.
- Outcome: Run effective automated scans and interpret results.

| 4 | **Manual Verification & Exploitation Basics** | 6 | CO4 |
|---|---|---|---|

- Why manual verification is needed; triaging scan results
- Exploitation vs proof-of-concept vs validation
- Safe exploit testing in lab environments (VMs, containers, CTF images)
- Tools: Metasploit for validation, Burp Suite for web verification, SQLmap basics
- Privilege escalation basics and impact analysis
- Practical component: Validate selected vulnerabilities using Metasploit and Burp.
- Outcome: Verify, validate and safely demonstrate real vulnerabilities.

| 5 | **Vulnerability Management & Remediation** | 5 | CO5 |
|---|---|---|---|

- Risk rating using CVSS and business context
- Prioritization frameworks (likelihood × impact)
- Patch management basics and change control interactions
- Mitigation strategies (configuration, compensating controls, WAFs)
- Re-scan cycles and verifying remediation
- Outcome: Convert findings into prioritized, actionable remediation plans.

| 6 | **Reporting, Metrics & Automation** | 4 | CO6 |
|---|---|---|---|

- Writing effective vulnerability assessment reports (executive summary, technical details, remediation steps)
- Remediation tracking and SLAs
- Key performance metrics (time-to-remediate, re-open rates, vulnerability backlog)
- Integrating VA into CI/CD & DevSecOps pipelines (automated scans, gating)
- Continuous monitoring and trending
- Outcome: Produce professional reports and integrate VA into organizational processes

## Reference Books


1. OWASP Testing Guide (latest).
2. The Web Application Hacker’s Handbook — Dafydd Stuttard & Marcus Pinto.
3. Nmap Network Scanning — Gordon 'Fyodor' Lyon.
4. Vendor docs: Nessus/OpenVAS user guides.
5. NVD (National Vulnerability Database) and CVE resources.
6. Recent industry whitepapers and research on VA trends.
7. The Basics of Hacking and Penetration Testing, by Patrick Engebretson, Released 2013, Publisher(s): Elsevier, ISBN: 9780124116443.
8. Metasploit: The Penetration Tester’s Guide, by David Kennedy, Jim O’Gorman, Devon Kearns, Mati Aharoni, Released July 2011, Publisher(s): No Starch Press, ISBN: 9781593272883.

9. Web Application Hacker's Handbook, by Dafydd Stuttard and Marcus Pinto, Released September 2011,
Publisher(s): Wiley Publishing, ISBN: 9781118026472.
10. Nmap Network Scanning, by Gordon Fyodor Lyon, Released January 2009,
Publisher(s): Insecure.Com LLC, ISBN: 9780979958717.

**E-Books and Online Learning Material**

1. **https://www.nist.gov/cyberframework?utm_source=chatgpt.com**
2. **https://www.nist.gov/cyberframework?utm_source=chatgpt.com**
3. **https://greenbone.github.io/docs/latest/?utm_source=chatgpt.com**

# Savitribai Phule Pune University
## B.Sc. Cyber Security
## Sem-V

### CYS-303-MJ-T: Basics of API Security Testing

| No. of Credits: 2 | Teaching Scheme<br>Theory: 2 Hrs/Week | Examination Scheme<br>Continuous Evaluation: 15 Marks<br>End Semester : 35 Marks |
|---|---|---|

**Prerequisites**

- Basics of networking, operating systems, and cybersecurity fundamentals

**Objectives**

- To understand the fundamentals of APIs, API architectures, and communication methods.
- To introduce students to REST, SOAP, and GraphQL APIs and their security challenges.
- To study common API vulnerabilities based on OWASP API Security Top 10.
- To develop practical skills in API security testing using industry-standard tools.
- To learn authentication and authorization testing techniques for APIs.
- To understand methods for identifying input validation, injection, and data exposure vulnerabilities.
- To perform basic vulnerability assessment and penetration testing of APIs.

**Course Outcomes**

On Completion of this course, student will be able to –

CO1: Know the architecture and working principles of modern APIs.

CO2: Understand authentication and authorization mechanisms in APIs.

CO3: Identify common vulnerabilities and their security implications.

CO4: Apply testing methodologies to assess API security posture.

CO5: Utilize tools to detect and interpret API vulnerabilities.

CO6: Recommend mitigation strategies and follow best practices for secure API development.

| Unit No. | Name of Unit | Teaching Hours | CO Targeted |
|---|---|---|---|
| **1** | **Introduction to API Security** | **5** | **CO1,CO2** |

- Overview of API concepts: REST, SOAP, GraphQL
- API architecture: client, server, endpoints, methods, and payloads
- Role of APIs in modern web and mobile applications
- Differences between Web App Security and API Security
- Common API authentication mechanisms: API Keys, OAuth 2.0, JWT
- API vulnerabilities vs traditional web vulnerabilities
- OWASP API Security Top 10 overview

| 2 | API Authentication and Authorization | 5 | CO2 |
|---|---|---|---|

- Authentication vs Authorization
- API Keys, Basic Auth, and Token-based Auth
- OAuth 2.0: Flow, Access Tokens, Refresh Tokens
- JSON Web Tokens (JWT): Structure, Signature, and Validation
- Common authentication flaws: Weak tokens, token reuse, session hijacking
- Broken Object Level Authorization (BOLA)
- Secure implementation of authorization at endpoint level

| 3 | Common API Vulnerabilities | 5 | CO3 |
|---|---|---|---|

- Injection flaws: SQL, NoSQL, Command injection
- Broken Authentication and Session Management
- Excessive Data Exposure
- Lack of Rate Limiting
- Mass Assignment and Insecure Deserialization
- Improper Assets Management
- Misconfigured Security Headers (CORS, CSP, TLS)
- Real-world case studies of API breaches

| 4 | API Security Testing Methodology | 5 | CO4 |
|---|---|---|---|

- API Testing Lifecycle: Discovery → Mapping → Testing → Reporting
- Reconnaissance: identifying endpoints and data flow
- Endpoint mapping and parameter analysis
- Testing inputs, headers, cookies, and authentication tokens
- Fuzzing and input validation testing concepts
- Handling responses and interpreting status codes
- Documentation analysis: Swagger/OpenAPI security checks
- Safe testing in non-production environments

| 5 | API Security Tools and Techniques | 5 | CO5 |
|---|---|---|---|

- Manual testing tools: Postman, Insomnia
- Interception and proxy tools: Burp Suite, OWASP ZAP
- Automated testing tools: Nikto, Nmap, APIsec, RESTler
- Token analysis: jwt.io, JWT Tool
- Common payloads and fuzzing concepts
- Logging, monitoring, and security testing automation in pipelines
- Interpreting results and avoiding false positives

| 6 | Reporting, Remediation, and Best Practices | 5 | CO6 |
|---|---|---|---|

- Structure of API Security Testing Report
- Risk rating using CVSS
- Writing vulnerability descriptions, impact analysis, and remediation guidance
- Secure coding guidelines for API developers
- Input validation and output encoding standards

- Importance of encryption (HTTPS, TLS, certificates)
- Secure DevOps (DevSecOps) integration for API lifecycle

## Reference Books


1. OWASP API Security Top 10 – https://owasp.org/www-project-api-security/
2. API Security in Action – Neil Madden
3. The Web Application Hacker's Handbook – Dafydd Stuttard & Marcus Pinto
4. OWASP Testing Guide (latest edition)
5. NVD (National Vulnerability Database) – https://nvd.nist.gov/
6. RFC 6749: OAuth 2.0 Authorization Framework


**E-Books and Online Learning Material**

- **https://owasp.org/API-Security/?utm_source=chatgpt.com**

**https://owasp.org/www-project-api-security/?utm_source=chatgpt.com**

# Savitribai Phule Pune University
# B.Sc. Cyber Security
# Sem-V

## CYS-304-MJ-T：Automation in Python for Cyber Security

| No. of Credits: | Teaching Scheme | Examination Scheme |
|---|---|---|
| 2 | Theory: 2 Hrs/Week | Continuous Evaluation: 15 Marks<br>End Semester : 35 Marks |

**Prerequisites**

- Basic knowledge of Python programming and computer networks

**Objectives**

- To understand the basics of Python programming for cybersecurity applications.
- To learn Python scripting for automating security and administrative tasks.
- To develop skills in file handling, log analysis, and network programming using Python.

**Course Outcomes**

CO1: Explain automation's role in cybersecurity operations.
CO2: Develop Python scripts for automating network and log analysis.
CO3: Perform automated web and API security testing using Python.
CO4: Use Python for malware detection and forensic analysis.
CO5: Create automated reports and alerts for cybersecurity workflows.

| Unit No. | Name of Unit | Teaching Hours | CO Targeted |
|---|---|---|---|
| 1 | **Introduction to Automation and Python Basics** | 5 | CO1 |

- Need for automation in Cyber Security
- Overview of scripting vs manual processes
- Introduction to Python environment setup
- Python modules and libraries for security
- File handling and OS operations
- Exception handling and logging
- Understanding APIs and command-line automation

| | | | |
|---|---|---|---|
| 2 | **Networking and Packet Analysis with Python** | 5 | CO2 |

- Networking modules: socket, ipaddress
- Creating simple port scanners using Python
- Packet capture and analysis using scapy
- Packet structure and headers
- Detecting suspicious traffic patterns
- Parsing pcap files for security events
- Simulating network testing (safe lab environment)

| | | | |
|---|---|---|---|
| 3 | **Log Analysis and File Monitoring Automation** | 6 | CO3 |

- Role of logs in cyber security
- Automating system log collection and parsing
- Using Regular Expressions for pattern matching

- Detecting anomalies and failed login attempts
- Monitoring changes in system files and directories
- Log correlation using Python
- Integration with SIEM tools

| 4 | **Web and API Automation for Security Testing** | **5** | **CO3** |
|---|---|---|---|

- Automating web requests using requests and urllib
- HTTP methods and response handling
- Extracting data using BeautifulSoup
- Automating login testing and brute-force detection
- API testing using Python scripts
- Validating input/output for vulnerabilities
- Basic integration with Burp Suite or OWASP ZAP APIs

| 5 | **Malware, Forensics, and Threat Automation** | **5** | **CO4** |
|---|---|---|---|

- Basics of malware analysis and sandboxing
- Automating hash generation (MD5, SHA1, SHA256)
- File integrity monitoring scripts
- Threat intelligence feeds automation (VirusTotal, AbuseIPDB APIs)
- Parsing JSON threat data
- Detecting suspicious processes and registry keys
- Automated forensic reporting concepts

| 6 | **Reporting, Scheduling, and Best Practices** | **5** | **CO5** |
|---|---|---|---|

- Automating report generation (CSV, Excel, PDF formats)
- • Email and alert automation
- • Task scheduling using schedule and cron
- • Logging and error handling in automated scripts
- • Security and ethical scripting practices
- • Version control and script maintenance
- • Secure coding and deployment considerations

## Reference Books


1. Violent Python – TJ O'Connor
2. Black Hat Python – Justin Seitz
3. Python for Cybersecurity – Packt Publishing
4. Automate the Boring Stuff with Python – Al Sweigart
5. Python for Offensive PenTest – Hussam Khrais
6. OWASP and MITRE ATT&CK documentation


## E-Books and Online Learning Material

- **https://docs.python.org/3/?utm_source=chatgpt.com**
- https://www.w3schools.com/python/?utm_source=chatgpt.com

# Savitribai Phule Pune University
# B.Sc. Cyber Security
# Sem-V

## CYS-305-MJ-P: Lab Course based on CYS-301-MJ-T & CYS-302-MJ-T

| **No. of Credits:** 2 | **Teaching Scheme** Practical: 4 Hrs/Week | **Examination Scheme** Continuous Evaluation: 15 Marks End Semester : 35 Marks |
|---|---|---|

**Prerequisites**

- Basic knowledge of Python programming and computer networks

**Objectives**

- To implement secure coding and defensive techniques.

**Course Outcomes**

CO1: To provide hands-on experience in web application security testing.
CO2: To understand common web vulnerabilities through practical demonstrations.
CO3: To implement secure coding and defensive techniques.
CO4: To develop professional web security testing and reporting skills.

| Practical No. | Title of Experiment | Teaching Hours | |
|---|---|---|---|
| 1 | **Installation and Setup of Web Security Lab Environment** | 5 | |
| | | | |
| 2 | **HTTP/HTTPS Traffic Analysis using Browser Developer Tools and Wireshark** | 10 | |
| | | | |
| 3 | **Web Application Mapping using Burp Suite** | 10 | |
| | | | |
| 4 | **Cross-Site Scripting (XSS) Attack and Prevention & SQL Injection Testing using SQLmap and Manual Techniques** | 15 | |
| | | | |
| 5 | **Web Vulnerability Scanning using Nikto and OWASP ZAP** | 10 | |
| | | | |
| 6 | **Vulnerability Scanning using OpenVAS & Exploitation Basics using Metasploit Framework** | 10 | |
| | | | |

# Savitribai Phule Pune University
## B.Sc. Cyber Security
## Sem-V
### CYS-306-MJ-P : Lab Course based on CYS-303-MJ-T & CYS-304-MJ-T

| **No. of Credits:** 2 | **Teaching Scheme** Practical: 4 Hrs/Week | **Examination Scheme** Continuous Evaluation: 15 Marks End Semester : 35 Marks |
|---|---|---|

**Prerequisites**

- Basic knowledge of computer networks and web technologies.
- Understanding of HTTP/HTTPS protocols and client-server architecture.

**Objective:**

- To understand API testing methods and vulnerabilities.
- To implement secure API handling and testing practices.
- To use Python for automation in cybersecurity tasks.
- To analyze, report, and mitigate API security issues using scripts and tools.

**Course Outcomes**

CO1: Test REST and SOAP APIs for security vulnerabilities.
CO2: Automate cybersecurity tasks using Python scripting.
CO3: Analyze and interpret API responses and vulnerabilities.
CO4: Write Python scripts for scanning, data collection, and automation.
CO5: Generate and document testing reports effectively.

| Practical No. | Name of Unit | Teaching Hours | CO Targeted |
|---|---|---|---|
| **1** | **API Security Testing** | **6** | **CO1** |
| **Objective:** Set up a testing environment for RESTful APIs and explore tools like Postman and Burp Suite.<br>**Tools:** Postman, Burp Suite, OWASP Juice Shop API | | | |
| **2** | **Practical 2: Authentication and Authorization Testing in APIs** | **6** | **CO1** |
| **Objective:** Test API endpoints using Basic Auth, Token-based Auth, and OAuth.<br>**Tools:** Postman, OWASP ZAP Learning Outcome: Students learn secure methods of managing users and protecting sessions. | | | |
| **3** | **Input Validation and Injection Testing** | **6** | **CO2** |
| • **Objective:** Identify input-based vulnerabilities such as SQL Injection and Command Injection in API endpoints.<br>**Tools:** Burp Suite, SQLMap XML External Entities (XXE)<br>• Case Studies: Famous Web Security Breaches<br>• Practical Component: Hands-on demonstration using DVWA / OWASP Juice Shop. | | | |
| **4** | **API Rate Limiting, Error Handling, and Information Disclosure Testing** | **6** | **CO3** |

- **Objective:** Test for improper rate limiting, verbose error messages, and sensitive data leaks.
  **Tools:** Postman, Burp Suite

| 5 | **Secure API Development and Reporting** | 6 | CO3, CO4 |
|---|---|---|---|

- **Objective:** Develop a simple Flask API with secure coding and generate a test report.
  **Tools:** Python (Flask), Postman

| B | **Section B — Automation in Python for Cyber Security** | 30 | CO4, CO5 |
|---|---|---|---|

**Practical 6:**
**Title:** Python Basics for Cyber Security
**Objective:** Write Python scripts for basic operations (file handling, data parsing, OS commands).
**Tools:** Python, Jupyter Notebook / VS Code

**Practical 7:**
**Title:** Network Scanning Automation using Python
**Objective:** Automate network scanning using Python scripts.
**Tools:** Python, socket, scapy libraries

**Practical 8:**
**Title:** Log Analysis and Threat Detection
**Objective:** Write Python scripts to read and analyze log files for suspicious activities.
**Tools:** Python, Regex

**Practical 9:**
**Title:** Web Scraping and Data Extraction for Threat Intelligence
**Objective:** Use Python to extract information from web sources for cybersecurity analysis.
**Tools:** Python, requests, BeautifulSoup

**Practical 10:**
**Title:** Vulnerability Scanner Automation (Mini Project)
**Objective:** Develop a simple Python-based vulnerability scanning script and generate a report.
**Tools:** Python, requests, nmap module

## Reference Books and Tools

- Postman / Burp Suite Community Edition
- OWASP ZAP
- OWASP Juice Shop (for API testing)
- Python 3.x
- Libraries: requests, os, socket, nmap, scapy, BeautifulSoup, json
- Flask / FastAPI (for secure API design)
- OWASP API Security Top 10 Guidelines
- PTES and NIST SP 800-115 (for structured testing approach)
- **https://owasp.org/www-project-top-ten/?utm_source=chatgpt.com**

# Savitribai Phule Pune University
## B.Sc. Cyber Security
## Sem-V

### CYS-310-MJ-T: Basics of Digital Forensic

| No. of Credits: 2 | Teaching Scheme<br>Theory: 2 Hrs/Week | Examination Scheme<br>Continuous Evaluation: 15 Marks<br>End Semester : 35 Marks |
|---|---|---|

**Prerequisites**

- Basic knowledge of computer networks and web technologies.
- Understanding of HTTP/HTTPS protocols and client-server architecture.

**Objective:**

- To introduce the fundamentals of digital forensics and investigation processes.
- To identify and preserve digital evidence for legal proceedings.
- To understand forensic tools, techniques, and ethical considerations.
- To perform basic forensic analysis on systems, networks, and mobile devices.

**Course Outcomes**

CO1: Explain digital forensic principles, tools, and investigation processes.

CO2: Identify and preserve digital evidence from different sources.

CO3: Use forensic tools to analyze computer and mobile data.

CO4: Prepare forensic reports and maintain evidence integrity.

CO5: Apply forensic techniques to solve cybercrime case studies.

| Unit No. | Name of Unit | Teaching Hours | CO Targeted |
|---|---|---|---|
| **1** | **Introduction to Digital Forensics** | **6** | **CO1** |

- Definition, Need, and Importance of Digital Forensics
- History and Evolution of Digital Forensics
- Categories: Computer, Network, Mobile, Cloud, and Database Forensics
- Role of Forensic Experts and Investigators
- Legal and Ethical Issues

| | | | |
|---|---|---|---|
| **2** | **Digital Evidence and Data Acquisition** | **6** | **CO2** |

- Types of Digital Evidence
- Chain of Custody and Documentation
- Evidence Collection Procedures
- Bit Stream Imaging and Verification
- Preservation of Volatile and Non-Volatile Data

| | | | |
|---|---|---|---|
| **3** | **File Systems and Data Recovery** | **6** | **CO3, CO4** |

- Understanding FAT, NTFS, EXT, and HFS+ File Systems
- Deleted File Recovery and Unallocated Space Analysis
- Metadata and Timestamps
- File Carving Techniques

- Use of Tools like Autopsy and FTK Imager

| 4 | **System and Network Forensics** | 6 | CO3, CO4 |
|---|---|---|---|

- Windows and Linux Forensics Basics
- Event Log and Registry Analysis
- Browser History and Cache Analysis
- Network Traffic Capturing and Analysis (Wireshark, TCPDump)
- Email Forensics

| 5 | **Mobile and Cloud Forensics** | 6 | CO3, CO4, CO5 |
|---|---|---|---|

- Mobile Device Structure and Data Extraction Techniques
- SIM, SD Card, and Application Data Analysis
- Cloud Storage Investigation
- Forensic Challenges in Virtualization and Cloud Environments
- Reporting and Case Documentation

## Reference Books


- Digital Forensics and Incident Response, by Gerard Johansen, Released June 2017, Publisher(s): Packt Publishing, ISBN: 9781783987467.
- Guide to Computer Forensics and Investigations, by Bill Nelson, Amelia Phillips, Christopher Steuart, Released January 2018, Publisher(s): Cengage Learning, ISBN: 9781337568944.
- Computer Forensics: Investigating Network Intrusions and Cyber Crime, by EC-Council, Released 2010, Publisher(s): Cengage Learning, ISBN: 9781435483521.
- File System Forensic Analysis, by Brian Carrier, Released March 2005, Publisher(s): Addison-Wesley Professional, ISBN: 9780321268174.
- Practical Mobile Forensics, by Satish Bommisetty, Heather Mahalik, and Rohit Tamma, Released December 2014, Publisher(s): Packt Publishing, ISBN: 9781783285198

# Savitribai Phule Pune University
## B.Sc. Cyber Security
## Sem-V

### CYS-311-MJ-P: Lab Course based on CYS-310-MJ-T

| No. of Credits: 2 | Teaching Scheme<br>Practical: 4 Hrs/Week | Examination Scheme<br>Continuous Evaluation: 15 Marks<br>End Semester : 35 Marks |
|---|---|---|

**Prerequisites**

- Basic knowledge of computer networks and web technologies.
- Understanding of HTTP/HTTPS protocols and client-server architecture.

**Objective:**

- To introduce the fundamentals of digital forensics and investigation processes.
- To identify and preserve digital evidence for legal proceedings.
- To understand forensic tools, techniques, and ethical considerations.
- To perform basic forensic analysis on systems, networks, and mobile devices.

**Course Outcomes**

1. CO1: Explain digital forensic principles, tools, and investigation processes.
2. CO2: Identify and preserve digital evidence from different sources.
3. CO3: Use forensic tools to analyze computer and mobile data.
4. CO4: Prepare forensic reports and maintain evidence integrity.
5. CO5: Apply forensic techniques to solve cybercrime case studies.

| Practical No. | Name of Practicals | Teaching Hours | CO Targeted |
|---|---|---|---|
| **1** | **Introduction to Digital Forensic Tools** | **12** | **CO1** |
| • Explore and install basic forensic tools (Autopsy, FTK Imager, Wireshark). | | | |
| **2** | **Disk Imaging and Verification & Network Traffic Capture and Analysis** | **12** | **CO2, CO3** |
| • Create a forensic image of storage media using FTK Imager and verify integrity using hash functions.<br>• Capture live network traffic using Wireshark and identify possible intrusions. | | | |
| **3** | **File Recovery and Deleted Data Analysis & Mobile Forensics Using Open-Source Tools** | **12** | **CO2, CO3** |
| • Recover deleted files and analyze recovered metadata. | | | |
| **4** | **Windows Log and Registry Analysis & Reporting and Documentation** | **12** | **CO4** |
| • Analyze event logs and registry entries for suspicious activities.<br>• Investigate artifacts from cloud services (Google Drive, Dropbox). | | | |

| 5 | **Browser and Email Forensics & Mini Project on Digital Investigation** | 12 | CO5 |
|---|---|---|---|

- Extract and interpret browsing history and email artifacts.
- Conduct an end-to-end forensic analysis (case simulation).

## Reference Books


- Digital Forensics and Incident Response, by Gerard Johansen, Released June 2017, Publisher(s): Packt Publishing, ISBN: 9781783987467.
- Guide to Computer Forensics and Investigations, by Bill Nelson, Amelia Phillips, Christopher Steuart, Released January 2018, Publisher(s): Cengage Learning, ISBN: 9781337568944.
- Computer Forensics: Investigating Network Intrusions and Cyber Crime, by EC-Council, Released 2010, Publisher(s): Cengage Learning, ISBN: 9781435483521.
- File System Forensic Analysis, by Brian Carrier, Released March 2005, Publisher(s): Addison-Wesley Professional, ISBN: 9780321268174.
- Practical Mobile Forensics, by Satish Bommisetty, Heather Mahalik, and Rohit Tamma, Released December 2014, Publisher(s): Packt Publishing, ISBN: 9781783285198

# Savitribai Phule Pune University
## B.Sc. Cyber Security
## Sem-V

### CYS-312-MJ-T: DevOps Fundamentals

| No. of Credits: | Teaching Scheme | Examination Scheme |
|---|---|---|
| 2 | Theory: 2 Hrs/Week | Continuous Evaluation: 15 Marks<br>End Semester : 35 Marks |

**Prerequisites**

- To understand DevOps concepts, tools, and lifecycle for continuous development and deployment.
- To integrate DevOps principles into secure software development environments.
- To automate deployment, configuration, and monitoring using modern tools.
- To implement CI/CD pipelines and Infrastructure as Code (IaC).

**Objective:**

- To introduce the fundamentals of digital forensics and investigation processes.
- To identify and preserve digital evidence for legal proceedings.
- To understand forensic tools, techniques, and ethical considerations.
- To perform basic forensic analysis on systems, networks, and mobile devices.

**Course Outcomes**

CO1: Explain DevOps concepts, benefits, and lifecycle.

CO2: Use Git and GitHub for version control and collaboration.

CO3: Implement automation using Jenkins, Docker, and Ansible.

CO4: Deploy applications using containerization and orchestration tools.

CO5: Integrate security practices into the DevOps pipeline (DevSecOps).

| Unit No. | Name of Unit | Teaching Hours | CO Targeted |
|---|---|---|---|
| **1** | **Introduction to DevOps** | **6** | **CO1** |

- Evolution of Software Development and Operations
- What is DevOps?
- Key Concepts and Principles of DevOps
- DevOps Lifecycle: Continuous Integration, Continuous Deployment, Continuous Monitoring
- Benefits and Challenges of DevOps
- DevSecOps Overview

| | | | |
|---|---|---|---|
| **2** | **Version Control Systems** | **6** | **CO2** |

- Introduction to Git and GitHub
- Repository, Branching, Merging, and Forking
- Git Commands and Workflow
- Managing Source Code and Collaboration

- CI Integration with GitHub

| 3 | **Continuous Integration and Continuous Deployment** | 6 | CO3 |
|---|---|---|---|

- Concept of CI/CD
- Jenkins Setup and Pipeline Configuration
- Automated Build, Test, and Deployment
- Integration with GitHub and Docker
- Role of CI/CD in Secure Development

| 4 | **Containerization and Orchestration** | 6 | CO4 |
|---|---|---|---|

- Introduction to Virtualization and Containers
- Docker Installation, Images, Containers, and Dockerfile
- Docker Compose and Networking
- Kubernetes Basics – Pods, Services, Deployments
- Container Security Concepts

| 5 | **Configuration Management and Monitoring** | 6 | CO5 |
|---|---|---|---|

- Infrastructure as Code (IaC)
- Ansible Basics – Playbooks, Inventory, Modules
- Monitoring Tools: Prometheus, Grafana
- Log Management and Alerts
- DevOps Security Best Practices

## Reference Books


- Len Bass, Ingo Weber, Liming Zhu — *DevOps: A Software Architect's Perspective*
- Gene Kim — *The Phoenix Project*
- Kief Morris — *Infrastructure as Code*
- Docker & Kubernetes Documentation
- Jenkins and Ansible Official Guides

# Savitribai Phule Pune University
## B.Sc. Cyber Security
## Sem-V

### CYS-313-MJ-P: Lab Course based on CYS-312-MJ-T

| No. of Credits: 2 | Teaching Scheme<br>Practical: 4 Hrs/Week | Examination Scheme<br>Continuous Evaluation: 15 Marks<br>End Semester : 35 Marks |
|---|---|---|

**Prerequisites**

- Basic knowledge of computer networks and web technologies.
- Understanding of HTTP/HTTPS protocols and client-server architecture.

**Objective:**

- To introduce the fundamentals of digital forensics and investigation processes.
- To identify and preserve digital evidence for legal proceedings.
- To understand forensic tools, techniques, and ethical considerations.
- To perform basic forensic analysis on systems, networks, and mobile devices.

**Course Outcomes**

CO1: Explain digital forensic principles, tools, and investigation processes.

CO2: Identify and preserve digital evidence from different sources.

CO3: Use forensic tools to analyze computer and mobile data.

CO4: Prepare forensic reports and maintain evidence integrity.

CO5: Apply forensic techniques to solve cybercrime case studies.

| Practical No. | Name of Practicals | Teaching Hours | CO Targeted |
|---|---|---|---|
| **1** | **Introduction to DevOps Tools and Setup & Version Control using Git and GitHub** | **12** | **CO1** |
| • Install and configure Git, Jenkins, Docker, and Ansible in a lab environment.<br>• Create repositories, manage branches, and perform merge operations. | | | |
| **2** | **Automating Build Process using Jenkins & Kubernetes Basics – Deployment and Scaling** | **12** | **CO2** |
| • Configure Jenkins and create a simple CI job linked with GitHub.<br>• Kubernetes Basics – Deployment and Scaling | | | |
| **3** | **Docker Basics – Containers and Images & Creating Dockerfiles and Using Docker Compose** | **12** | **CO3** |
| • Create, run, and manage Docker containers for sample applications.<br>• Build custom Docker images and deploy multi-container applications. | | | |

| | | | |
|---|---|---|---|
| **4** | **Continuous Deployment using Jenkins and Docker & Configuration Management with Ansible** | **12** | **CO4** |
| • Write Ansible playbooks to automate system configuration.<br>• Automate application deployment pipeline with Jenkins and Docker. | | | |
| **5** | **Monitoring and Logging in DevOps & Mini Project – End-to-End DevOps Pipeline** | **12** | **CO5** |
| • Build a secure CI/CD pipeline integrating Git, Jenkins, Docker, and Ansible.<br>• Use Prometheus or Grafana for real-time application monitoring. | | | |
| | | | |

## Reference Books


- Len Bass, Ingo Weber, Liming Zhu — *DevOps: A Software Architect's Perspective*
- Gene Kim — *The Phoenix Project*
- Kief Morris — *Infrastructure as Code*
- Docker & Kubernetes Documentation
- Jenkins and Ansible Official Guides

# Savitribai Phule Pune University
## B.Sc. Cyber Security
## Sem-V

### CYS-321-VSC: Embedded Systems

| No. of Credits: 2 | Teaching Scheme<br>Theory: 2 Hrs/Week | Examination Scheme<br>Continuous Evaluation: 15 Marks<br>End Semester : 35 Marks |
|---|---|---|

**Prerequisites**

- Basic knowledge of computer organization and digital electronics.
- Understanding of programming concepts using C/C++ language.

**Objective:**

- To understand the fundamentals and architecture of embedded systems.
- To learn microcontroller design and functioning.
- To explore communication protocols and interfacing techniques.
- To understand applications of embedded systems in cybersecurity and IoT.

**Course Outcomes**

CO1: Explain the architecture and working of embedded systems.

CO2: Describe microcontrollers, sensors, and communication interfaces.

CO3: Analyze embedded applications used in IoT and cybersecurity.

CO4: Understand real-time operating systems and firmware basics.

CO5: Evaluate security aspects of embedded devices.

| Unit No. | Name of Unit | Teaching Hours | CO Targeted |
|---|---|---|---|
| **1** | **Introduction to Embedded Systems** | **6** | **CO1** |

- Definition and Characteristics of Embedded Systems
- Embedded vs General Purpose Systems
- Design Challenges and Real-Time Constraints
- Embedded System Lifecycle
- Applications in Cybersecurity, IoT, and Industrial Automation

| | | | |
|---|---|---|---|
| **2** | **Architecture of Embedded Systems** | **6** | **CO2** |

- Basic Components: Processor, Memory, Input/Output Devices
- Types of Processors: Microcontroller, Microprocessor, DSP
- Harvard vs Von Neumann Architectures
- Memory Organization and Buses
- Embedded System Hardware Blocks

| | | | |
|---|---|---|---|
| **3** | **Microcontrollers and Programming Concepts** | **6** | **CO3** |

- Overview of 8051, ARM, Arduino, and Raspberry Pi
- GPIO, Timers, Interrupts, and Peripheral Devices
- Embedded C and MicroPython Overview

- Compilation, Uploading, and Debugging Process
- Firmware Design and Real-Time Execution

| 4 | **Interfacing and Communication Protocols** | 6 | CO4 |
|---|---|---|---|

- Sensor and Actuator Basics
- Data Conversion: ADC and DAC
- Communication Interfaces: UART, SPI, I2C
- Display Devices (LCD, LED, OLED)
- Wireless Modules: Wi-Fi, Bluetooth, ZigBee

| 5 | **Embedded Systems in Cyber Security and IoT** | 6 | CO5 |
|---|---|---|---|

- Role of Embedded Systems in IoT
- Common Security Threats and Vulnerabilities in Embedded Devices
- Secure Boot, Encryption, and Firmware Protection
- Case Study: IoT-Based Smart Security System
- Future Directions in Embedded and Secure System Design

## Reference Books


- Raj Kamal — *Embedded Systems: Architecture, Programming, and Design*
- Frank Vahid & Tony Givargis — *Embedded System Design: A Unified Hardware/Software Introduction*
- Mazidi — *The 8051 Microcontroller and Embedded Systems*
- Elecia White — *Making Embedded Systems*
- Arduino & Raspberry Pi Official Documentation

# Savitribai Phule Pune University
## B.Sc. Cyber Security
## Sem-V

### CYS-331-FP: Project on Cyber Security

| No. of Credits: | Teaching Scheme | Examination Scheme |
|---|---|---|
| 2 | Practical: 4 Hrs/Week | Continuous Evaluation: 15 Marks<br>End Semester : 35 Marks |

**Prerequisites**

- Basic knowledge of computer organization and digital electronics.
- Understanding of programming concepts using C/C++ language.

**Objective:**

- To enable students to practically apply cybersecurity concepts and tools.
- To develop problem-solving and research-based project skills.
- To strengthen project documentation, teamwork, and presentation abilities.
- To create awareness about professional ethics and innovation in cybersecurity.

**Course Outcomes**

CO1: Identify a practical or research-oriented cybersecurity problem.

CO2: Design and implement a small-scale project or prototype.

CO3: Apply cybersecurity tools, languages, or frameworks for real-world solutions.

CO4: Prepare project documentation and present findings effectively.

1. **Type of Project:**
    - Mini or applied project related to cybersecurity, networking, IoT, or automation.
    - Can be **individual** or **group-based** (maximum 2–3 students).
2. **Duration:**
    - Total workload equivalent to **30 hours** per semester.
3. **Supervision:**
    - Each project should be guided by a faculty member.
4. **Project Stages:**
    - **Phase I:** Problem Identification & Synopsis Submission
    - **Phase II:** System Design & Implementation
    - **Phase III:** Final Presentation & Viva

## Suggested Project Areas:

- Web or API Security Testing
- Network Scanning Automation
- IoT Device Security
- Log Analysis for Threat Detection
- Malware Simulation and Defense
- Cloud Security Implementation
- Python Automation for Cyber Tasks
- Vulnerability Assessment Tools
- Digital Forensics Evidence Analyzer
- Secure Communication Application

| | |
|---|---|
| Project Synopsis / Proposal | 10 |
| Project Report & Documentation | 15 |
| Working Model / Implementation | 15 |
| Presentation & Viva | 10 |
| **Total** | **50 Marks** |

## Suggested Tools and Platforms:

- Programming Languages: Python, C/C++, Java
- Cyber Tools: Kali Linux, Burp Suite, OWASP ZAP, Wireshark
- IoT Tools: Arduino, Raspberry Pi
- Cloud Platforms: AWS / Azure / Google Cloud
- Report Tools: MS Word, LaTeX, Google Docs

# Savitribai Phule Pune University
## B.Sc. Cyber Security
## Sem-V

### CYS-341-MN-T: Internet of Things for Cyber Security

| No. of Credits: | Teaching Scheme | Examination Scheme |
|---|---|---|
| 2 | Theory: 2 Hrs/Week | Continuous Evaluation: 15 Marks<br>End Semester : 35 Marks |

**Prerequisites**

- Basic knowledge of computer networks and web technologies.
- Understanding of HTTP/HTTPS protocols and client-server architecture.

**Objective:**

- To introduce the fundamentals of digital forensics and investigation processes.
- To identify and preserve digital evidence for legal proceedings.
- To understand forensic tools, techniques, and ethical considerations.
- To perform basic forensic analysis on systems, networks, and mobile devices.

**Course Outcomes**

CO1: Explain IoT architecture and its core building blocks.

CO2: Identify and analyze IoT communication protocols.

CO3: Understand and mitigate IoT-related cybersecurity threats.

CO4: Evaluate and apply IoT security frameworks and standards.

| Unit No. | Name of Unit | Teaching Hours | CO Targeted |
|---|---|---|---|
| 1 | **Introduction to IoT** | 6 | CO1 |

- Definition and Characteristics of IoT
- IoT Components: Devices, Gateways, Cloud, and Applications
- Evolution and Importance of IoT in Modern Systems
- IoT Applications in Smart Homes, Healthcare, and Industry
- Role of IoT in Cyber Security

| 2 | **IoT Architecture and Communication Models** | 6 | CO2 |
|---|---|---|---|

- 3-Layer and 5-Layer IoT Architectures
- IoT Functional Blocks and Sensors
- IoT Communication Models: Device-to-Device, Device-to-Cloud, Gateway-Based
- IoT Networking Technologies: RFID, NFC, Bluetooth, ZigBee, Wi-Fi, LoRaWAN
- Cloud and Edge Computing in IoT

| 3 | **IoT Communication Protocols** | 6 | CO3 |
|---|---|---|---|

- Overview of IoT Protocol Stack
- Application Layer Protocols: MQTT, CoAP, HTTP, AMQP
- Transport and Network Layer: TCP, UDP, IPv6, 6LoWPAN

- Security Features of Common IoT Protocols
- Case Study: MQTT Security Implementation

| 4 | **IoT Security Challenges and Threats** | 6 | CO4 |
|---|---|---|---|

- Vulnerabilities in IoT Devices and Networks
- Common IoT Attacks: DDoS, Botnets, Firmware Exploits, Side-Channel Attacks
- Authentication and Access Control in IoT
- Data Privacy, Integrity, and Encryption Techniques
- Risk Assessment and Mitigation Strategies

| 5 | **Secure IoT Design and Future Trends** | 6 | CO3, CO4 |
|---|---|---|---|

- Secure IoT Development Life Cycle
- Security Standards: OWASP IoT Top 10, ISO/IEC 27030
- Secure Boot and Firmware Update Mechanisms
- Blockchain and AI Integration in IoT Security
- Future Trends: Smart Cities, Industrial IoT, and Edge AI

**Reference Books**


- Arshdeep Bahga & Vijay Madisetti — *Internet of Things: A Hands-On Approach*
- Raj Kamal — *Internet of Things: Architecture and Design Principles*
- Alan Bensky — *Short-Range Wireless Communication*
- Qusay F. Hassan — *Internet of Things: Challenges, Advances, and Applications*
- OWASP IoT Project Documentation

# Detail Syllabus
# B.Sc. (Cyber Security)
# Semester-VI

# Savitribai Phule Pune University
## B.Sc. Cyber Security
## Sem-VI

### CYS-351-MJ-T: Windows Terminal for Cyber Security

| No. of Credits: 2 | Teaching Scheme<br>Theory: 2 Hrs/Week | Examination Scheme<br>Continuous Evaluation: 15 Marks<br>End Semester : 35 Marks |
|---|---|---|

**Prerequisites**

- Basic knowledge of Windows OS, command-line operations, and cybersecurity concepts.

**Objective:**

- To introduce the fundamentals of digital forensics and investigation processes.
- To identify and preserve digital evidence for legal proceedings.
- To understand forensic tools, techniques, and ethical considerations.
- To perform basic forensic analysis on systems, networks, and mobile devices.

**Course Outcomes**

CO1: Configure and securely use Windows Terminal with PowerShell and WSL for cybersecurity tasks.
CO2: Use PowerShell and CLI tools to inspect system, network, and process states.
CO3: Extract and analyze logs to build basic forensic timelines using terminal tools.
CO4: Write scripts to automate data collection, triage, and remediation tasks.
CO5: Harden terminal/shell configurations and detect malicious script activity.
CO6: Apply ethical and secure practices when using terminal tools for investigations

| Unit No. | Name of Unit | Teaching Hours | CO Targeted |
|---|---|---|---|
| 1 | **Introduction to Windows Terminal and Shells** | 5 | CO1, CO2 |

- Overview of Windows Terminal: features, UI (tabs, panes, profiles, settings)
- Differences between Command Prompt, PowerShell, and WSL (bash)
- Installing and configuring Windows Terminal (profiles, keybindings, themes)
- Terminal security basics (secure profiles, execution policies)
- Common terminal workflows in security operations

| 2 | **PowerShell Essentials for Security** | 5 | CO2 |
|---|---|---|---|

- PowerShell fundamentals: cmdlets, objects, and pipelines
- Execution policy, modules, and profiles
- Working with files, registry, processes, and services
- PowerShell remoting and WinRM basics (security considerations)
- Security features: Constrained Language Mode, AMSI, script signing

| 3 | **CLI Tools & Windows Sysinternals** | 5 | CO2 |
|---|---|---|---|

- Using built-in CLI tools: netstat, tasklist, ipconfig, route, sc, wevtutil, wmic
- Introduction to Sysinternals Suite (Process Explorer, Autoruns, Procmon, PsExec, TCPView)
- Integrating Sysinternals tools via PowerShell/Terminal
- Reading and filtering Windows Event Logs (wevtutil & Get-WinEvent)
- Network and process forensics using CLI tools

| 4 | **Log Analysis, Parsing & Forensics in Terminal** | **5** | **CO3, CO4** |
|---|---|---|---|

- Understanding Windows Event Logs: authentication, application, system logs
- Querying and filtering logs using PowerShell (Get-WinEvent, Select-String)
- Parsing logs using regex and PowerShell pipelines
- Analyzing IIS and application logs in terminal
- Timeline building and forensic triage using terminal workflows

| 5 | **Automation, Scripting & Incident Response Workflows** | **5** | **CO4, CO5** |
|---|---|---|---|

- Writing PowerShell scripts for security automation
- Automating scans, alerts, and data collection (Task Scheduler)
- Using Terminal for IR workflows (collect, analyze, remediate)
- Safe remote collection with PSRemoting, SMB, WinRM, and SFTP
- Integrating with SIEM/APIs using PowerShell
- Hardening Terminal and shells: secure settings, profile separation
- Detecting malicious PowerShell activity (logging, AMSI, transcription)

| 6 | **Advanced Topics, Hardening & Best Practices** | **5** | **CO5, CO6** |
|---|---|---|---|

- Hardening Terminal and shells: secure settings, profile separation
- Detecting malicious PowerShell activity (logging, AMSI, transcription)
- WSL security considerations and Linux tooling on Windows
- Red-team vs blue-team terminal use (ethical aspects)
- Credential handling, secret management, and secure logging

## Reference Books


- Microsoft Docs: PowerShell, Windows Terminal, Event Logs, and WinRM.
- Sysinternals Suite – Mark Russinovich (Microsoft).
- PowerShell for Sysadmins – Adam Bertram.
- Windows Forensics and Incident Recovery – select chapters on CLI workflows.
- OWASP and SANS whitepapers on PowerShell abuse and defenses.
- Microsoft Security Blog – Defender and AMSI integration updates.

# Savitribai Phule Pune University
## B.Sc. Cyber Security
## Sem-VI

### CYS-352-MJ-T: PowerShell basics

| No. of Credits: 2 | Teaching Scheme<br>Theory: 2 Hrs/Week | Examination Scheme<br>Continuous Evaluation: 15 Marks<br>End Semester : 35 Marks |
|---|---|---|

**Prerequisites**

- Basic knowledge of Windows Operating System and Command Line Interface.

**Objective:**

- To introduce the fundamentals of digital forensics and investigation processes.
- To identify and preserve digital evidence for legal proceedings.
- To understand forensic tools, techniques, and ethical considerations.
- To perform basic forensic analysis on systems, networks, and mobile devices.

**Course Outcomes**

CO1: Understand PowerShell architecture and command structure.
CO2: Execute and automate administrative tasks using cmdlets and scripts.
CO3: Write structured PowerShell scripts for automation.
CO4: Manage system configurations, network settings, and user accounts.
CO5: Use PowerShell in security monitoring and forensic analysis.
CO6: Apply PowerShell as a cyber defense tool to identify and respond to threats.

| Unit No. | Name of Unit | Teaching Hours | CO Targeted |
|---|---|---|---|
| **1** | **Introduction to PowerShell** | **5** | **CO1** |

- Overview of PowerShell and its evolution
- PowerShell vs Command Prompt
- PowerShell editions and versions (Windows PowerShell vs PowerShell Core)
- Understanding cmdlets, scripts, and pipelines
- PowerShell console and Integrated Scripting Environment (ISE)
- Basic commands for file and system navigation

| | | | |
|---|---|---|---|
| **2** | **Working with Cmdlets and Objects** | **5** | **CO2** |

- Structure and syntax of cmdlets
- Using Get-Command, Get-Help, and Get-Member
- Working with objects, properties, and methods
- Piping and chaining commands
- Formatting outputs (Format-Table, Format-List, Select-Object)

- Sorting, filtering, and exporting data (Sort-Object, Where-Object, Export-CSV)

| 3 | **PowerShell Scripting Fundamentals** | 5 | CO3 |
|---|---|---|---|

- Writing and running PowerShell scripts (.ps1 files)
- Variables, data types, and operators
- Conditional statements (if, else, switch)
- Loops (for, foreach, while, do-while)
- Functions and parameters
- Script execution policy and digital signatures

| 4 | **System Administration using PowerShell** | 5 | CO4 |
|---|---|---|---|

- Managing files, folders, and drives
- Process and service management (Get-Process, Stop-Service, etc.)
- Managing users and groups (local machine)
- Registry manipulation and system configuration
- Scheduling tasks and automating administrative actions
- Querying system information and performance data

| 5 | **PowerShell for Networking and Security** | 5 | CO5 |
|---|---|---|---|

- PowerShell networking cmdlets (Test-Connection, Get-NetIPAddress, Get-NetTCPConnection)
- Retrieving and analyzing network configurations
- PowerShell Remoting (Enable-PSRemoting, Enter-PSSession)
- Managing firewall settings via PowerShell
- Introduction to security modules (Get-ExecutionPolicy, Set-ExecutionPolicy)
- Generating system and security audit reports

| 6 | **PowerShell in Cyber Security Operations** | 5 | CO6 |
|---|---|---|---|

- PowerShell as a tool in Cyber Security
- Gathering forensic artifacts using PowerShell
- Monitoring event logs and user activity
- Detecting malicious processes and network activity
- PowerShell in incident response and digital forensics
- Defensive scripting and preventing misuse of PowerShell

## Reference Books


- *Learn Windows PowerShell in a Month of Lunches* – Don Jones & Jeffrey Hicks.
- *Windows PowerShell Cookbook* – Lee Holmes.
- *PowerShell in Depth* – Don Jones, Jeffrey Hicks, and Richard Siddaway.
- *Microsoft Docs: PowerShell Overview and Command Reference.*
- *PowerShell for Cybersecurity* – SANS Institute Whitepapers.
- *PowerShell and Active Directory Administration Guide* – Microsoft Learn.

# Savitribai Phule Pune University
## B.Sc. Cyber Security
## Sem-VI

### CYS-353-MJ-T: Fundamentals of Active Directory

| No. of Credits: | Teaching Scheme | Examination Scheme |
|---|---|---|
| 2 | Theory: 2 Hrs/Week | Continuous Evaluation: 15 Marks<br>End Semester : 35 Marks |

**Prerequisites**

- Basic knowledge of Computer Networks
- Understanding of Operating Systems (Windows/Linux)
- Fundamentals of Cyber Security
- Basic knowledge of Client-Server Architecture
- Familiarity with TCP/IP and DNS concepts

**Objective:**

- To introduce the concepts and architecture of Active Directory services.
- To understand domain structures, organizational units, users, groups, and policies in Active Directory.
- To learn authentication, authorization, and access control mechanisms in Windows environments.
- To understand Group Policy Management and security configurations in enterprise networks.
- To study Active Directory security threats, monitoring, and best practices for secure administration.

**Course Outcomes**

CO1: Understand the architecture and components of Active Directory services
CO2: Configure and manage domains, users, groups, and organizational units
CO3: Apply authentication and authorization mechanisms using Active Directory
CO4: Implement Group Policies and security configurations in enterprise environments.
CO5: Analyze Active Directory security risks and recommend protection mechanisms.

| Unit No. | Name of Unit | Teaching Hours | CO Targeted |
|---|---|---|---|
| 1 | **Introduction to Active Directory** | 6 | |

- Fundamentals of Active Directory
- Evolution of Directory Services
- Active Directory Architecture
- Domains, Trees, Forests, and Sites
- Domain Controllers and Roles
- Active Directory Services Overview

| | | | |
|---|---|---|---|
| 2 | **Active Directory Objects and Management** | 6 | |

- Users, Groups, and Computers
- Organizational Units (OUs)
- Creating and Managing User Accounts
- Group Types and Scopes
- Active Directory Administrative Tools
- Delegation of Administrative Control

| 3 | **Authentication and Access Control** | **6** | |
|---|---|---|---|

- Kerberos Authentication Protocol
- LDAP Fundamentals
- NTLM Authentication
- Access Control Lists (ACLs)
- User Authentication and Authorization
- Password Policies and Account Security

| 4 | **Group Policy and Security Management** | **6** | |
|---|---|---|---|

- Introduction to Group Policy Objects (GPOs)
- Group Policy Processing
- Managing Security Policies
- Software Deployment using GPO
- Auditing and Monitoring in Active Directory
- Backup and Recovery Concepts

| 5 | **Active Directory Security and Best Practices** | **6** | |
|---|---|---|---|

- Active Directory Security Threats
- Privilege Escalation and Misconfigurations
- Active Directory Attack Techniques Overview
- Security Hardening Techniques
- Best Practices for AD Administration
- Introduction to Hybrid Identity and Azure AD

## Reference Books


- Mastering Active Directory – Packt Publishing.
- Active Directory Administration Cookbook – Packt Publishing.
- Windows Server Administration Fundamentals – Wiley Publications.
- Active Directory for Dummies – Wiley Publishing.
- Windows Server 2022 & PowerShell All-in-One For Dummies – Wiley Publishing.
- Identity with Windows Server 2016 – Microsoft Press.

# Savitribai Phule Pune University
## B.Sc. Cyber Security
## Sem-VI

### CYS-354-MJ-T: Penetration Testing

| No. of Credits: 2 | Teaching Scheme<br>Theory: 2 Hrs/Week | Examination Scheme<br>Continuous Evaluation: 15 Marks<br>End Semester : 35 Marks |
|---|---|---|

**Prerequisites**

- Fundamentals of networking, operating systems, basic web technologies, and cybersecurity concepts

**Objective:**

- Understand what PT is, different approaches, legal/ethical boundaries, and industry frameworks.
- Be able to plan and perform comprehensive, ethical information gathering and map attack surface.
- Know how to discover and prioritize vulnerabilities and enumerate services and accounts.
- Understand common exploitation vectors, their impact, and how to safely validate findings.

**Course Outcomes**

CO1: Describe PT methodologies, legal/ethical constraints, and testing scopes.
CO2: Collect and analyze reconnaissance data to map attack surfaces.
CO3: Use scanning and enumeration theory to identify and prioritize vulnerabilities.
CO4: Explain common exploitation techniques and their impact on systems and web apps.
CO5: Understand post-exploitation objectives and defensive countermeasures.
CO6: Prepare professional penetration test reports with prioritized remediation guidance.

| Unit No. | Name of Unit | Teaching Hours | CO Targeted |
|---|---|---|---|
| **1** | **Introduction to Penetration Testing** | **5** | **CO1** |

- Definition, scope and objectives of penetration testing
- Types: Black-box, White-box, Grey-box
- PT methodology & phases (Planning → Recon → Scanning → Exploitation → Post-exploitation → Reporting)
- Legal, ethical, and contractual considerations (scope, rules of engagement, permissions)
- Risk, vulnerability vs exploit, CVE/CVSS basics
- PT frameworks and standards (OSSTMM, PTES, NIST)

| | | | |
|---|---|---|---|
| **2** | **Reconnaissance & Footprinting** | **5** | **CO2** |

- Passive reconnaissance: OSINT sources, domain/IP discovery, WHOIS, Google dorking
- Active reconnaissance basics: ping, DNS enumeration, banner grabbing concepts
- Asset identification and attack surface mapping
- Profiling technologies (web server, CMS, frameworks)

- Social engineering overview (conceptual) and data gathering ethics

| 3 | **Scanning, Enumeration & Vulnerability Discovery** | 5 | CO3 |
|---|---|---|---|

- Network scanning concepts: host discovery, port scanning, service detection
- Vulnerability scanning types and tuning (authenticated vs unauthenticated)
- Enumeration: SMB, LDAP, SNMP, web directories, user enumeration concepts
- Interpreting scan results and reducing false positives
- Vulnerability databases & exploit search (NVD, Exploit-DB basics)

| 4 | **Exploitation Techniques & Web App Testing** | 5 | CO4 |
|---|---|---|---|

- Exploitation fundamentals and exploit development concepts (high-level)
- Common web application attacks: SQLi, XSS, CSRF, file upload, authentication bypasses
- Command injection, RCE, file inclusion, path traversal concepts
- Safe testing principles and use of exploit frameworks (conceptual: Metasploit)
- Demonstration-level theory of payloads and shells (no hands-on)

| 5 | **Post-Exploitation, Privilege Escalation & Lateral Movement6** | 5 | CO5 |
|---|---|---|---|

- Post-exploitation goals: persistence, data access, pivoting, cleanup (ethics!)
- Windows and Linux privilege escalation strategies (theory): misconfigurations, SUID, weak permissions, unpatched services
- Credential harvesting, Kerberos basics, pass-the-hash/pass-the-ticket concepts (overview)
- Lateral movement techniques and segmentation importance
- Evidence handling, forensic implications of PT activities

| 6 | **Reporting, Risk Management & Defence Recommendations** | 5 | CO6 |
|---|---|---|---|

- Structure of a professional PT report: executive summary, technical findings, PoC, remediation steps, risk rating
- Prioritization using CVSS and business context; communicating to technical and non-technical stakeholders
- Remediation advice: configuration, patches, controls, WAF, network segmentation
- Metrics for PT programs and retest cycles
- Integrating PT with secure SDLC and continuous security testing

## Reference Books


- PTES (Penetration Testing Execution Standard) — ptes.org
- OWASP Testing Guide & OWASP Top 10 (for web testing) — owasp.org
- *The Web Application Hacker's Handbook* — Stuttard & Pinto (for theory)
- *Metasploit: The Penetration Tester's Guide* — conceptual reading (no lab required)
- NVD / CVE databases; Exploit-DB for exploit descriptions
- NIST SP 800-115: Technical Guide to Information Security Testing and Assessment

# Savitribai Phule Pune University
## B.Sc. Cyber Security
## Sem-VI

### CYS-355-MJ-P: Lab Course based on CYS-351-MJ-T & CYS-352-MJ-T

| **No. of Credits:** 2 | **Teaching Scheme** Practical: 4 Hrs/Week | **Examination Scheme** Continuous Evaluation: 15 Marks End Semester : 35 Marks |
|---|---|---|

**Prerequisites**

- Fundamentals of networking, operating systems, basic web technologies, and cybersecurity concepts

**Objective:**

- To provide practical knowledge of Windows administration and management.
- To introduce automation through PowerShell scripting for system administration.
- To enhance cybersecurity awareness and defensive skills in Windows environments.
- To prepare students for professional tasks in system and security administration

**Course Outcomes**

CO1: Perform essential Windows administrative operations.
CO2: Configure, monitor, and secure Windows systems.
CO3: Automate administrative and cybersecurity tasks using PowerShell.
CO4: Develop simple PowerShell scripts for managing users, files, and processes.
CO5: Implement automation for monitoring and reporting system performance

## Guidelines

- Students must perform **practical assignments** (Windows and PowerShell).
- Each practical must include **commands, screenshots, and result explanations**.
- Final evaluation includes **a mini project** and **viva** based on both sections.

**Section A – Windows Practicals**

| No. | Practical Title |
|---|---|
| 1 | Explore Windows interface, Control Panel, Device Manager, and System Tools. |
| 2 | Configure and test Windows Firewall and Defender Security options |
| 3 | Create and manage disk partitions and perform backup & restore operations |
| 4 | Monitor system performance using Task Manager and Resource Monitor |
| 5 | Create and manage disk partitions and perform backup & restore operations |
| 6 | Optional: Configure local security policy and user access controls |

## Section B – PowerShell Practicals

| No. | Practical Title |
|---|---|
| 1 | Introduction to PowerShell environment and basic cmdlets (Get-Help, Get-Command, etc.). |
| 2 | Write a PowerShell script to manage files, folders, and permissions. |
| 3 | Create and delete user accounts using PowerShell commands. |
| 4 | Automate system information collection (IP, CPU, RAM details). |
| 5 | Write a PowerShell script to monitor running services and export report to file. |
| 6 | Optional: Mini Project – Automate security audit tasks using PowerShell. |

## Tools and Environment

- **Operating System:** Windows 10 / 11
- **Utilities:** Control Panel, Task Manager, Computer Management
- **Scripting Tool:** PowerShell 5.1 or 7+
- **Optional:** Virtual Machine for testing, VS Code / PowerShell ISE

## Recommended Resources


1. Don Jones & Jeffrey Hicks — *Learn Windows PowerShell in a Month of Lunches*
2. Microsoft Documentation — *Windows Administration & PowerShell Reference*
3. Ed Wilson — *Windows PowerShell Step by Step*
4. Microsoft Learn — *Windows System Management & Security Modules*
5. TutorialsPoint — *Windows and PowerShell for Beginners*

# Savitribai Phule Pune University
## B.Sc. Cyber Security
## Sem-VI

### CYS-356-MJ-P: Lab Course based on CYS-353-MJ-T & CYS-354-MJ-T

| **No. of Credits:** 2 | **Teaching Scheme** Practical: 4 Hrs/Week | **Examination Scheme** Continuous Evaluation: 15 Marks End Semester : 35 Marks |
|---|---|---|

**Prerequisites**

- Fundamentals of networking, operating systems, basic web technologies, and cybersecurity concepts

**Objective:**

- To provide hands-on experience in setting up and managing Active Directory environments.
- To develop practical skills in penetration testing and ethical hacking tools.
- To understand security configurations, access control, and network exploitation.
- To apply cybersecurity principles in securing and testing real-world systems.

**Course Outcomes**

CO1: Configure and manage users, groups, and policies in Active Directory.

CO2: Implement authentication, authorization, and access control mechanisms.

CO3: Use penetration testing tools to identify vulnerabilities.

CO4: Perform reconnaissance, scanning, exploitation, and reporting.

CO5: Demonstrate ethical and responsible use of security testing tools

**Guidelines**

- Students must perform practical assignments (on Active Directory + on Penetration Testing).
- Each practical should include commands, configurations, screenshots, and result explanations.
- Mini-project or case-based test recommended at semester end

**Section A – Active Directory Practicals**

1. Install and configure Active Directory Domain Services on Windows Server
2. Create and manage users, groups, and organizational units (OUs).
3. Implement Group Policy Objects (GPOs) for system and user configurations
4. Configure authentication and password policies
5. Manage user permissions and shared resources using access control
6. Backup and restore Active Directory objects

**Section B – Penetration Testing Practicals**

1. Introduction to Kali Linux and ethical hacking lab setup.
2. Perform network scanning using Nmap and identify open ports.
3. Conduct vulnerability assessment using OpenVAS or Nessus.
4. Perform web application testing using OWASP ZAP or Burp Suite
5. Exploit a test system using Metasploit Framework and generate a report.
6. Wireless network security testing using Aircrack-ng suite

**Tools and Environment**

- Active Directory Tools: Windows Server 2016/2019, AD DS, Group Policy Editor
- Penetration Testing Tools: Kali Linux, Nmap, Burp Suite, Metasploit, OWASP ZAP, OpenVAS
- Virtualization: VirtualBox / VMware for Lab Setup
- Documentation Tools: Word / Markdown for Reports

**Recommended Resources**


1. Brian Svidergol — Active Directory Administration Cookbook
2. Microsoft Learn — Active Directory and Group Policy Management
3. Dafydd Stuttard & Marcus Pinto — The Web Application Hacker's Handbook
4. Georgia Weidman — Penetration Testing: A Hands-On Introduction to Hacking
5. OWASP Documentation and Kali Linux Official User Guide

# Savitribai Phule Pune University
## B.Sc. Cyber Security
## Sem-VI

### CYS-360-MJ-T: Advanced Digital Forensic

| No. of Credits: 2 | Teaching Scheme<br>Theory: 2 Hrs/Week | Examination Scheme<br>Continuous Evaluation: 15 Marks<br>End Semester : 35 Marks |
|---|---|---|

**Prerequisites**

- Fundamentals of networking, operating systems, basic web technologies, and cybersecurity concepts

**Objective:**

- To understand advanced techniques of digital evidence collection and analysis.
- To explore forensic tools and methods used in cybercrime investigations.
- To apply forensic techniques to real-world scenarios and case studies.
- To strengthen analytical and reporting skills in digital forensic processes.

**Course Outcomes**

CO1: Explain advanced concepts of digital evidence acquisition and preservation.

CO2: Use forensic tools for data recovery and system investigation.

CO3: Analyze forensic data from various devices and environments.

CO4: Prepare professional forensic reports with integrity and authenticity.

CO5: Demonstrate hands-on experience through practical forensic exercises.

| Unit No. | Name of Unit | Teaching Hours | CO Targeted |
|---|---|---|---|
| 1 | **Introduction to Advanced Digital Forensics** | 6 | CO1 |

- Review of Digital Forensics Fundamentals
- Digital Evidence and Cybercrime Overview
- Chain of Custody and Legal Considerations
- Stages of Forensic Investigation
- Challenges in Modern Forensics

| | | | |
|---|---|---|---|
| 2 | **Forensic Acquisition and Preservation** | 6 | CO2 |

- Forensic Imaging and Cloning Techniques
- Data Integrity and Hash Functions (MD5, SHA1, SHA256)
- Volatile and Non-Volatile Data Acquisition
- Evidence Handling Procedures
- Case Study: Disk Image Analysis

| | | | |
|---|---|---|---|
| 3 | **File System and Data Analysis** | 6 | CO3 |

- File System Structures: FAT, NTFS, EXT, HFS+
- Recovering Deleted Files and Hidden Data
- Memory and Log File Analysis

- Metadata and Timestamp Analysis
- Tools: Autopsy, FTK Imager, X-Ways

| 4 | **Network and Mobile Forensics** | 6 | CO4 |
|---|---|---|---|

- Basics of Network Forensics and Packet Capture
- Log Analysis and Traffic Reconstruction
- Mobile Device Data Extraction Techniques
- SIM, SD Card, and App-Level Analysis
- Tools: Wireshark, Cellebrite, Oxygen Forensic Suite

| 5 | **Cloud and Advanced Forensic Techniques** | 6 | CO4, CO5 |
|---|---|---|---|

- Challenges in Cloud Forensics
- Remote Evidence Collection
- Anti-Forensic Techniques and Countermeasures
- Reporting, Documentation, and Expert Testimony
- Emerging Trends in AI-Based Forensics

## Reference Books


- Eoghan Casey — *Digital Evidence and Computer Crime*
- Nelson, Phillips, Steuart — *Guide to Computer Forensics and Investigations*
- Maras — *Cybercrime and Digital Forensics*
- Kruse & Heiser — *Computer Forensics: Incident Response Essentials*
- Official Documentation of Autopsy, FTK, and Wireshark

# Savitribai Phule Pune University
## B.Sc. Cyber Security
## Sem-VI

### CYS-361-MJ-P: Lab Course based on CYS-360-MJ-T

| **No. of Credits:** 2 | **Teaching Scheme** Practical: 4 Hrs/Week | **Examination Scheme** Continuous Evaluation: 15 Marks End Semester : 35 Marks |
|---|---|---|

**Prerequisites**

- Fundamentals of networking, operating systems, basic web technologies, and cybersecurity concepts

**Objectives:**

- To understand advanced techniques of digital evidence collection and analysis.
- To explore forensic tools and methods used in cybercrime investigations.
- To apply forensic techniques to real-world scenarios and case studies.
- To strengthen analytical and reporting skills in digital forensic processes.

**Course Outcomes**

CO1: Explain advanced concepts of digital evidence acquisition and preservation.

CO2: Use forensic tools for data recovery and system investigation.

CO3: Analyze forensic data from various devices and environments.

CO4: Prepare professional forensic reports with integrity and authenticity.

CO5: Demonstrate hands-on experience through practical forensic exercises.

## Guidelines

- Students should perform **practical assignments** covering forensic tools and techniques.
- Each practical must include **screenshots, analysis reports, and findings**.
- One **mini project or case investigation** must be completed at the end of the semester.

**Practical Assignments**

1. Perform disk imaging using FTK Imager or Autopsy.
2. Recover deleted files from storage media.
3. Analyze Windows event logs and system registry for evidence
4. Perform memory dump and analyze using Volatility Framework
5. Conduct file system forensic analysis (FAT/NTFS).
6. Capture and analyze network packets using Wireshark
7. Perform email header and attachment analysis.
8. Mobile device data extraction using open-source tools
9. Cloud data investigation (Google Drive / AWS sample case).

10. Mini Project: Complete forensic case study with full report

## Tools and Software Suggested

- **Forensic Tools:** Autopsy, FTK Imager, Volatility, Wireshark, EnCase (demo)
- **Mobile Tools:** Cellebrite UFED, MOBILedit, Oxygen Forensic Suite
- **Platforms:** Windows, Linux (Kali), Virtual Machines for testing

## Recommended Books


1. Eoghan Casey — *Digital Evidence and Computer Crime*
2. Nelson, Phillips, Steuart — *Guide to Computer Forensics and Investigations*
3. Maras — *Cybercrime and Digital Forensics*
4. Kruse & Heiser — *Computer Forensics: Incident Response Essentials*
5. Official Documentation of Autopsy, FTK, and Wireshark

# Savitribai Phule Pune University
## B.Sc. Cyber Security
## Sem-VI

### CYS-362-MJ-T: DevSecOps Fundamentals

| No. of Credits: 2 | Teaching Scheme<br>Theory: 2 Hrs/Week | Examination Scheme<br>Continuous Evaluation: 15 Marks<br>End Semester : 35 Marks |
|---|---|---|

**Prerequisites**

- Basic knowledge of software development life cycle (SDLC).
- Understanding of operating systems and computer networks.

**Objective:**

- To understand the principles of DevOps and its security integration (DevSecOps).
- To explore tools and practices that automate and secure the software development lifecycle (SDLC).
- To apply continuous integration and deployment (CI/CD) pipelines with embedded security.
- To perform hands-on practicals for secure coding, automation, and vulnerability scanning.

**Course Outcomes**

CO1: Explain DevOps lifecycle and integration of security (DevSecOps).

CO2: Use automation tools to implement CI/CD pipelines.

CO3: Identify and mitigate vulnerabilities in code, containers, and cloud environments.

CO4: Apply security tools within CI/CD for compliance and monitoring.

CO5: Develop a mini secure pipeline for software deployment.

| Unit No. | Name of Unit | Teaching Hours | CO Targeted |
|---|---|---|---|
| **1** | **Introduction to DevOps and DevSecOps** | **6** | **CO1** |

- DevOps fundamentals and SDLC phases
- Key components: CI, CD, automation, and collaboration
- Need for integrating security (DevSecOps)
- DevSecOps principles: “Shift Left Security”
- Culture, people, process, and tools

| | | | |
|---|---|---|---|
| **2** | **DevSecOps Lifecycle & Architecture** | **6** | **CO1** |

- Secure Software Development Lifecycle (SSDLC)
- Stages: Plan → Code → Build → Test → Release → Deploy → Operate → Monitor
- Automation in security testing
- Integrating security in DevOps pipelines
- Case study: CI/CD pipeline with security gates

| | | | |
|---|---|---|---|
| **3** | **Tools and Platforms** | **6** | **CO2, CO3** |

- Git, GitHub, Jenkins, Docker, Kubernetes overview

- Security Tools: SonarQube, OWASP Dependency-Check, Trivy, Snyk
- Infrastructure as Code (IaC) with Ansible and Terraform
- Container Security and Image Scanning
- Cloud Security basics (AWS / Azure pipelines)

| 4 | **Security Testing in CI/CD** | 6 | CO4 |
|---|---|---|---|

- Static Application Security Testing (SAST)
- Dynamic Application Security Testing (DAST)
- Software Composition Analysis (SCA)
- Secrets management (Vault, environment variables)
- Security monitoring and incident response integration.

| 5 | **Best Practices and Compliance** | 6 | CO5 |
|---|---|---|---|

- Secure coding practices and automation
- Logging and auditing DevOps activities
- Continuous compliance and governance
- DevSecOps metrics and KPIs
- Emerging trends: AI in DevSecOps, Zero Trust Pipelines

## Reference Books


- Gene Kim et al. — *The DevOps Handbook*
- Jim Bird — *DevSecOps: Building Security into DevOps*
- AWS Whitepapers — *DevSecOps Implementation Guide*
- OWASP Foundation — *DevSecOps Best Practices*
- Official Documentation of Jenkins, Docker, SonarQube, and Trivy

# Savitribai Phule Pune University
## B.Sc. Cyber Security
## Sem-VI

### CYS-363-MJ-P: Lab Course based on CYS-362-MJ-T

| **No. of Credits:** 2 | **Teaching Scheme** Theory: 4 Hrs/Week | **Examination Scheme** Continuous Evaluation: 15 Marks End Semester: 35 Marks |
|---|---|---|

**Prerequisites**

- Fundamentals of networking, operating systems, basic web technologies, and cybersecurity concepts

**Objective:**

- To understand the principles of DevOps and its security integration (DevSecOps).
- To explore tools and practices that automate and secure the software development lifecycle (SDLC).
- To apply continuous integration and deployment (CI/CD) pipelines with embedded security.
- To perform hands-on practicals for secure coding, automation, and vulnerability scanning.

**Course Outcomes**

CO1: Explain DevOps lifecycle and integration of security (DevSecOps).
CO2: Use automation tools to implement CI/CD pipelines.
CO3: Identify and mitigate vulnerabilities in code, containers, and cloud environments.
CO4: Apply security tools within CI/CD for compliance and monitoring.
CO5: Develop a mini secure pipeline for software deployment.

## Guidelines

- Perform **practical assignments** focused on integrating security in DevOps tools.
- Maintain **screenshots, reports, and explanations** in a journal.
- Final **mini project** to create a secure CI/CD pipeline with security tools integrated.

## Practical Assignments

1. Install and configure Git and Jenkins on local or cloud environment
2. Create a basic CI/CD pipeline in Jenkins for a sample web app
3. Integrate SonarQube for code quality and vulnerability scanning
4. Perform SAST and DAST testing using OWASP tools.
5. Implement containerization using Docker and image scanning with Trivy.
6. Deploy a secure container using Kubernetes (Minikube or Docker Desktop)

7. Automate deployment using Ansible or Terraform.
8. Integrate security testing tools (e.g., OWASP Dependency-Check) in CI/CD pipeline
9. Manage secrets securely using HashiCorp Vault or Jenkins credentials plugin
10. Mini Project: Build a secure CI/CD pipeline integrating Jenkins, Docker, and SonarQube

## Tools & Software

- **Version Control:** Git, GitHub
- **CI/CD:** Jenkins, GitLab CI, GitHub Actions
- **Security Tools:** SonarQube, Trivy, OWASP ZAP, Dependency-Check
- **Container Tools:** Docker, Kubernetes
- **Automation Tools:** Ansible, Terraform
- **Cloud Platforms:** AWS, Azure (optional labs)

## Recommended Books / Resources


1. Gene Kim et al. — *The DevOps Handbook*
2. Jim Bird — *DevSecOps: Building Security into DevOps*
3. AWS Whitepapers — *DevSecOps Implementation Guide*
4. OWASP Foundation — *DevSecOps Best Practices*
5. Official Documentation of Jenkins, Docker, SonarQube, and Trivy

# Savitribai Phule Pune University
## B.Sc. Cyber Security
## Sem-VI

### CYS-371-VSC: Embedded System Programming

| No. of Credits: 2 | Teaching Scheme<br>Practical: 4 Hrs/Week | Examination Scheme<br>Continuous Evaluation: 15 Marks<br>End Semester : 35 Marks |
|---|---|---|

**Prerequisites**

- Fundamentals of networking, operating systems, basic web technologies, and cybersecurity concepts

**Objective:**

- To provide hands-on experience in embedded system programming and interfacing.
- To understand microcontroller-based system development and IoT integration.
- To learn programming for sensors, actuators, and communication modules.
- To apply embedded system concepts for security and automation applications.

**Course Outcomes**

After successful completion of this course, students will be able to:

CO1: Write and execute embedded programs using microcontrollers.

CO2: Interface sensors, actuators, and displays with controllers.

CO3: Implement communication protocols such as UART, I2C, and SPI.

CO4: Develop mini-projects using Arduino or ESP32 boards.

CO5: Apply embedded programming concepts in cybersecurity or IoT domains.

**Guidelines**

- Perform **following practical assignments** (mandatory).
- Maintain **journal records** with circuit diagrams, code listings, output screenshots, and explanations.
- At the end, each student must complete a **mini-project or case study** based on embedded applications.

## Tools and Hardware

- **Development Boards:** Arduino Uno / ESP32 / Raspberry Pi (optional)
- **Sensors:** DHT11, PIR, IR, LDR, Ultrasonic, etc.
- **Software:** Arduino IDE / MicroPython / Tinkercad (simulation)
- **Connectivity:** Wi-Fi, Serial Monitor, USB

## List of Practical Assignments

| No. | Title of Practical / Experiment |
|---|---|
| 1 | Introduction to Arduino IDE and programming basics. |
| 2 | Write a program to blink LED using Arduino/ESP32. |
| 3 | Interfacing push button and controlling output device. |
| 4 | Interfacing temperature or humidity sensor (e.g., DHT11). |
| 5 | Display sensor data on serial monitor or LCD. |
| 6 | Interfacing motion sensor (PIR) for detecting movement. |
| 7 | Implement serial communication between Arduino and computer. |
| 8 | Interfacing buzzer and controlling it using conditions. |
| 9 | Build a simple IoT-based security alert system (with Wi-Fi module). |
| 10 | Mini Project: Design an embedded application for home or network security. |

## Recommended Resources


1. Simon Monk — *Programming Arduino: Getting Started with Sketches*
2. Massimo Banzi — *Getting Started with Arduino*
3. Dr. Raj Kamal — *Embedded Systems: Architecture, Programming and Design*
4. Espressif Documentation — *ESP32 Developer Guide*
5. Arduino Official Tutorials — https://www.arduino.cc/en/Tutorial/HomePage

# Savitribai Phule Pune University
## B.Sc. Cyber Security
## Sem-VI

### CYS-381-OJT: On Job Training (Internship)

| No. of Credits: | Teaching Scheme | Examination Scheme |
|---|---|---|
| 4 | Practical: 8 Hrs/Week | Continuous Evaluation: 30 Marks<br>End Semester : 70 Marks |

## Prerequisites:

- Basic knowledge of Computer Networks and Cyber Security concepts
- Understanding of Operating Systems and Networking fundamentals
- Familiarity with programming/scripting basics
- Knowledge of cyber security tools and safe computing practices
- Completion of Second Year B.Sc. (Cyber Security) coursework

**Objective:**

- To provide students with practical exposure to cyber security tools, technologies, and industrial practices.
- To enable students to apply theoretical cyber security concepts in real-world environments.
- To develop analytical thinking, ethical hacking awareness, and security problem-solving abilities.
- To encourage teamwork, communication, and professional interaction within cyber security domains.
- To familiarize students with industry standards, cyber laws, and secure working practices.

**Course Outcomes**

**CO1:** Enhance knowledge related to cyber security tools, technologies, and industrial practices.
**CO2:** Analyze and solve security-related problems using appropriate techniques and methodologies.
**CO3:** Apply critical thinking and analytical skills to identify and mitigate cyber threats.
**CO4:** Demonstrate effective communication and teamwork skills while working with industry experts and mentors
**CO5:** Gain practical experience in cyber security projects, security auditing, or related industry work
**CO6:** Prepare professional documentation including design, implementation, testing, and security reports
**CO7**: Understand industry-specific cyber security standards, policies, and compliance requirements.
**CO8**: Complete assigned projects/tasks successfully within predefined objectives and timelines

## Guidelines for On Job Training:

- Students are expected to complete cybersecurity-related work/projects within 120 hours assigned by the organization (company/industry/consultancy/institution).

- Students can start the OJT/Internship immediately after completion of Sem V (Fulltime in vacation period) or during Sem VI (Parttime after lecture/practical hours).
- The internship work may involve cybersecurity assignments such as vulnerability assessment, penetration testing, security monitoring, network security, incident response, digital forensics, security auditing, secure software development, cloud security, or equivalent work.
- The college should assign mentors/guides to students for monitoring progress throughout the OJT.
- Students must submit weekly progress reports duly signed by concerned authorities of the organization to the assigned mentor.
- At the end of OJT, students should prepare documentation and submit the internship report to the college in the prescribed format.
- After completion of OJT, final presentation and documentation shall be evaluated by the examination panel as per university norms
- Students must follow ethical practices, confidentiality policies, and cybersecurity guidelines of the organization during the internship period.